Securing the Smart Grid: Issues and Answers

Paul Halpin, AVP – Global Utility Lead
Science Applications International Corporation (SAIC)

June 26, 2009

SAIC
From Science to Solutions

10-0865

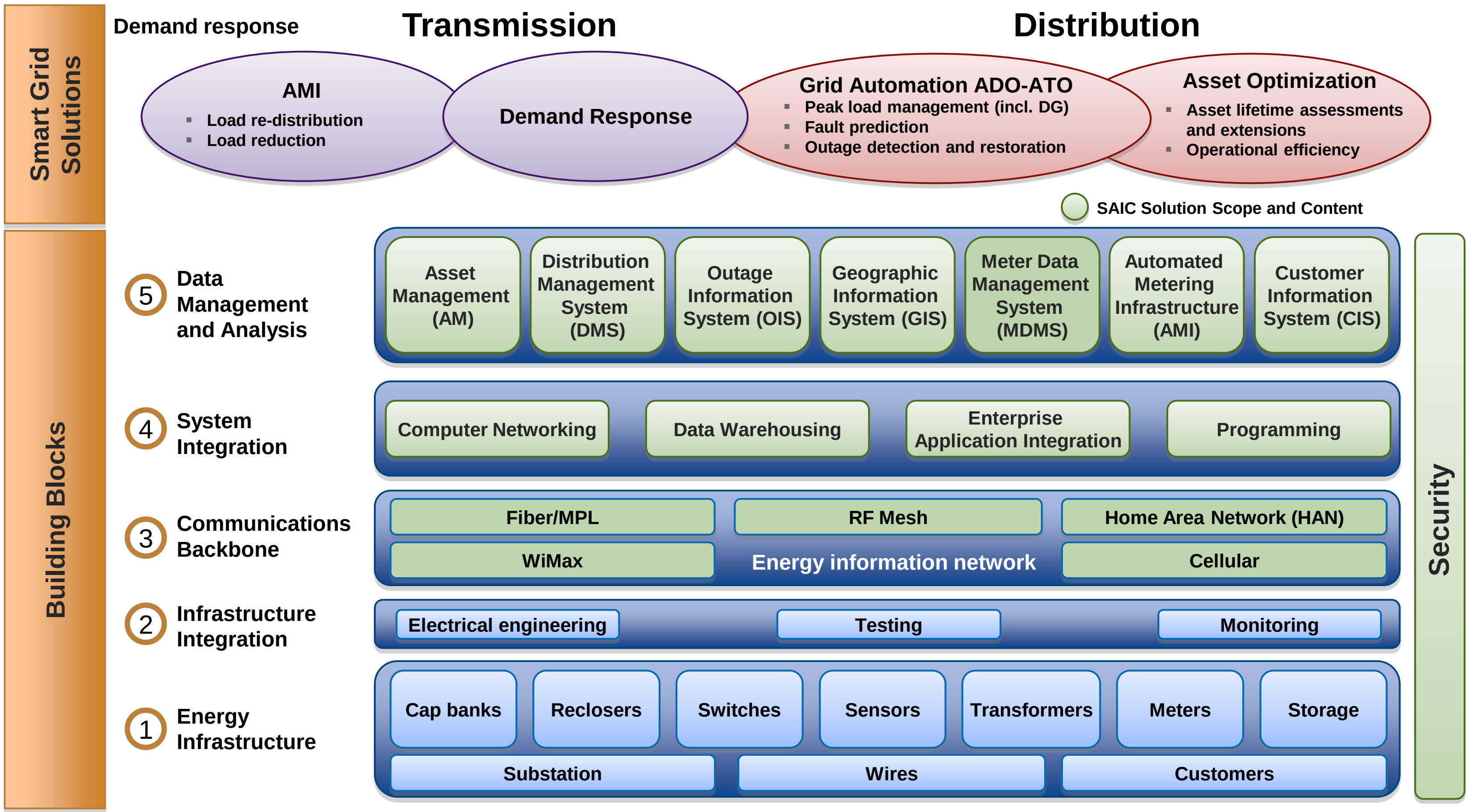
Risk & Security Challenges

- As defined in the 2006 Department of Homeland Security National Infrastructure Protection Plan (NIPP) :

  "**Cyber Infrastructure** includes electronic information and communication systems, and the information contained in those systems. Computer systems, control systems such as **Supervisory Control and Data Acquisition (SCADA)** systems, and networks such as the Internet are all part of the cyber infrastructure."
- Networked utility instrumentation and communication infrastructure bring security concerns that did not previously exist:
  - Exposed critical infrastructure control processes
  - Increased threats and attack focus on SCADA systems
  - Greater need to understand, track, remediate vulnerabilities
  - Data protection and data privacy concerns, because delivery occurs over a common infrastructure
- Risk = Threats x Vulnerabilities x Consequences
- In a converging and interconnected world, our risk continues to rise almost exponentially as all three risk factors continue to grow
- Smart Grid and AMI are classic examples

SAIC
From Science to Solutions

Typical Smart Grid IT Solution Architecture



AMI = advanced metering infrastructure ADO-ATO = advanced distribution operations-advanced transmission operations DG = distributed generation MPL = municipal power and light RF = radio frequency WiMax = worldwide interoperability for microwave access

SAIC From Science to Solutions

Why Securing the Grid Is a TOP Priority

- The U.S. is under cyber attack virtually all the time, every day
- Cyber-terrorists see the electric grid as a high-impact target
- The electric infrastructure is highly dependent on computer-based control systems that are used to monitor and manage sensitive processes and physical functions

WCBS is a registered trademark of CBS Broadcasting Inc. in the U.S. and/or other countries.

From Science to Solutions

Threats Constantly Evolving

- **1981:** Kevin Mitnick cracks PacBell and steals passwords
- **1986:** Pakistani Brain virus (first malicious virus)
- **1988:** Morris Worm released (first Internet worm)
- **1991:** Michelangelo virus
- **1995:** Web site defacements
- **1999:** Melissa worm
- **2000:** Distributed denial of service (DDoS) attacks
- **2005:** Microsoft Office® exploits
- **2006:** SCADA exploit tool
- **2007:** Estonia cyber riots
- **2007:** Pentagon computer system attacked
- **2008:** Georgia cyber riots
- **2009:** Downandup virus infected 10 million systems (and growing) and could become a botnet

Microsoft Office is a registered trademark of Microsoft Corporation in the United States and/or other countries.
SCADA = Supervisory Control and Data Acquisition

SAIC® From Science to Solutions

Critical Infrastructure Targeted

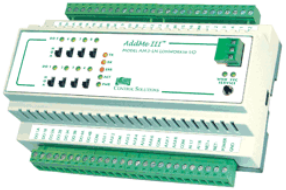
- **1998:** Telephone switch hack closes an airport
- **2000:** Gazprom central control is hacked
- **2000:** Australian hacker causes environmental harm by releasing sewage
- **2001:** Hackers protesting U.S./China conflict enter U.S. electric power systems
- **2001:** World Trade Center is attacked(?)
- **2003:** Power outages in northeastern United States occur
- **2003:** Worm shuts systems down at Davis-Besse nuclear plant
- **2006:** Zotob virus shuts down Holden car manufacturing plant

- The list continues to grow ----

SAIC®
From Science to Solutions

Vendor and equipment diversity

- AMI, MDM, SCADA and Grid product vendors offer a multitude of Smart Grid products and equipment.
- With diversity comes a broad range of proprietary tools and widely diverse security capabilities and limitations.
- Growing diversity translates into complexity, cost and vulnerabilities as utilities struggle to impose cohesive security models across the broad range of intelligent products that comprise a Smart Grid power landscape.
- Clear lack of standards



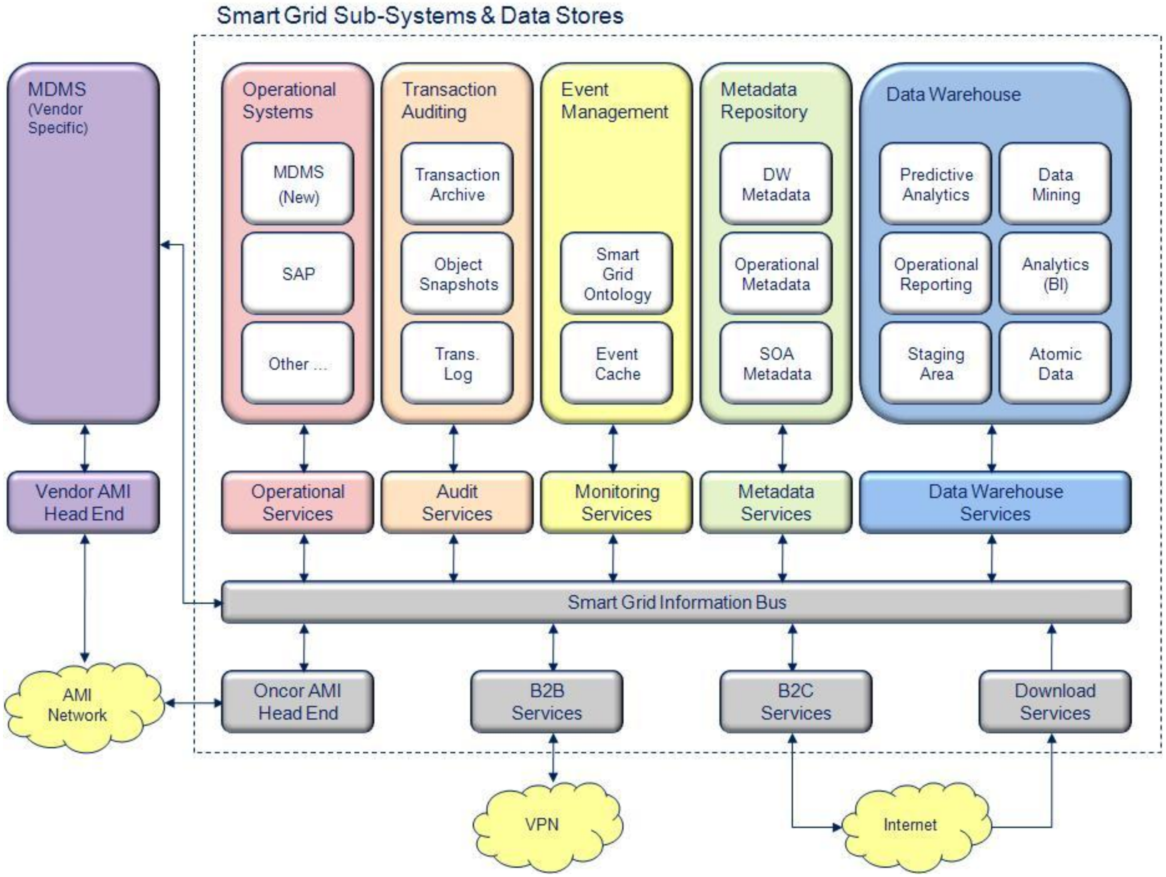
AMI = advanced metering infrastructure MDM = meter data management SCADA = supervisory control and data acquisition

Smart Grid security framework and strategic design goals

- **A common security model** – A platform- and vendor-independent security framework that seamlessly binds heterogeneous grid elements under a "common security model"
- **Transparency** – A framework that is "transparent" to heterogeneous, intelligent, grid-resident devices and to data center-resident advanced metering infrastructure/meter data management system applications and utility systems
- **A common interaction model** – A framework that provides a common, consistent model for secure grid device and data center system interaction, regardless of client capabilities or limitations
- **Proven, standards-based foundation** – A framework fully based upon proven, powerful and forward-looking industry security standards

From Science to Solutions

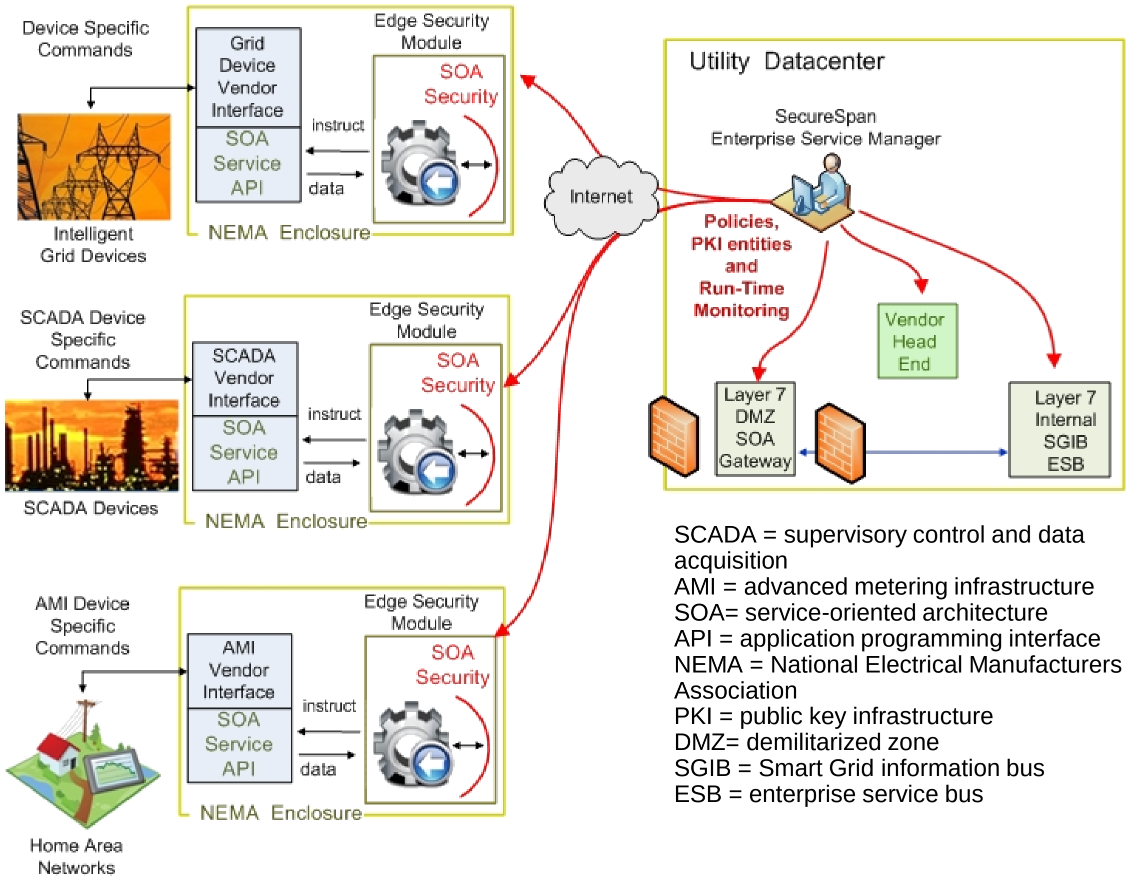
Smart Grid / AMI – Environment



- **Address the complexity, security and data issues associated with a Smart Grid / AMI implementation**
- **Implement secure communication technologies**
- **Integrate applications utilizing open standards and secure open source technologies**
- **Address the inherent security issues associated with vendor applications**
- **The Energy Utility "Edge Event Module" … Solution provides an intelligent and impenetrable 'air-gap' between IP addressable Smart Grid / AMI components devices (e.g. data aggregators and Head-end systems)**

Smart Grid Security:

Addressing Challenges



SCADA = supervisory control and data acquisition
AMI = advanced metering infrastructure
SOA= service-oriented architecture
API = application programming interface
NEMA = National Electrical Manufacturers Association
PKI = public key infrastructure
DMZ= demilitarized zone
SGIB = Smart Grid information bus
ESB = enterprise service bus

Framework: key concepts

- Wrap and abstract key grid device APIs.
- Expose a common, powerful security model.
- Enforce security through a common, powerful embedded security engine.
- Adaptive, declarative integration with abstracted devices.
- Keep grid device abstraction (the “edge security module”) very low cost
- Central grid and data center governance

SAIC From Science to Solutions

The Take Away's

- This is a critical national infrastructure, and unambiguous success is highly unlikely
- Increased mandates may actually encourage less security by moving focus to compliance, not security
- Vendor assumptions and utility assumptions are often poorly aligned
- There is a clear need to address both the message transport layer / infrastructure, and the 'system edge' components (meters, collectors etc.)
- Major transformation programs tend to focus on technical security capabilities and all but ignore process and procedure
- Capability discussions tend to be technology focused, not risk and impact focused
- Organizational and political barriers limit the integration of information and management
- Success may be better defined as, "Your ability to identify and respond to emerging threats."

SAIC® From Science to Solutions